EXPLICIT CLASSIFICATION FOR TORSION SUBGROUPS OF RATIONAL POINTS OF ELLIPTIC CURVES

Derong QIU and Xianke ZHANG
(Department of Mathematics, Tsinghua University,
Beijing 100084, P. R. China)

Abstract. The classification of elliptic curves E over the rationals $\mathbb{Q}$ is studied according to their torsion subgroups $E_{tors}(\mathbb{Q})$ of rational points. Explicit criteria for the classification are given when $E_{tors}(\mathbb{Q})$ are cyclic groups with even orders. The generator points P of $E_{tors}(\mathbb{Q})$ are also explicitly presented in each case. These results, together with recent results of K. Ono, completely solve the problem of the mentioned explicit classification when E has a rational point of order 2.

1991 Mathematical Subject Classification: 11G05, 14H52, 14K05
Keywords: elliptic curve, rational point, torsion group, arithmetic algebraic geometry

I. Introduction and Main Results

Let E be an elliptic curve defined over the rationals $\mathbb{Q}$. We consider the following two problems here: How to determine the rational torsion subgroup from the equation of E ? How to obtain the generator of the rational torsion subgroup explicitly?

From the Mordell-Weil theorem , we know that the Mordell-Weil group $E(\mathbb{Q})$ is a finitely generated abelian group having the form

$$E(\mathbb{Q}) \cong E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$$

where $E(\mathbb{Q})$ is the group of the $\mathbb{Q}$-rational points of E, $E_{tors}(\mathbb{Q})$ is the torsion subgroup of $E(\mathbb{Q})$ ($i.e.$, all points of $E(\mathbb{Q})$ with finite order), $\mathbb{Z}$ the rational intergers.

In 1977, B. Mazur completely determined all the possible types of the rational torsion group $E_{tors}(\mathbb{Q})$ in [1-2]. He shew that the torsion subgroup must be one of the following fifteen groups:

$$\mathbb{Z}/N\mathbb{Z} \qquad (1 \leq N \leq 10 \quad \textbf{o}r \quad N = 12);$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \qquad (1 \leq N \leq 4).$$

And each of these groups does occur as an $E_{tors}(\mathbb{Q})$ for some E (see [4], p223).

Recently, K.Ono in [3] studied the first problem above in an aspect. When torsion subgroups $E_{tors}(\mathbb{Q})$ are not cyclic, he gave criteria to classify them. In fact, K. Ono considered elliptic curves E with $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which could be assumed to have the equation $E: \quad y^2 = x(x+M)(x+N)$, with $M,\ N \in \mathbb{Z}$. He obtained necessary and sufficient conditions on $M,\ N$ for the torsion subgroup to be each of the following types respectively:

(1) $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; **(2)** $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$;
(3) $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

We here will consider the case that the torsion subgroups $E_{tors}(\mathbb{Q})$ are cyclic with even order, and will solve the two problems mentioned in the beginning.

Suppose that

$$E: \quad y^2 = f(x)$$

is an elliptic curve, $f(x) \in \mathbb{Q}[x]$. Assume that $f(x)$ has three complex roots $\alpha,\ \beta,\ \gamma$, then $P_1 = (\alpha, 0),\ P_2 = (\beta,\ 0),\ P_3 = (\gamma,\ 0)$ are just the three non-trival points of order two of E. So $E[2] = \{O, P_1, P_2, P_3\}$ are the group of torsion points of order two of E. By Mazur theorem, $E_{tors}(\mathbb{Q})$ is not cyclic if and only if $E_{tors}(\mathbb{Q}) \supset E[2]$; *i.e.*, $\alpha,\ \beta,\ \gamma \in \mathbb{Q}$. From this we deduce that $E_{tors}(\mathbb{Q})$ is cyclic if and only if $f(x)$ has at most one rational root. Thus we know that $E_{tors}(\mathbb{Q})$ is cyclic with even order if and only if E has just one non-trival rational point of order 2; that is, $f(x)$ has just one rational root. Let us assume so. Then, up to a translation, we may assume this rational root of $f(x)$ to be 0; so we have $f(x) = x(x-\alpha)(x-\beta)$. Since $\alpha+\beta$ and $\alpha\beta$ are rationals, we have $\alpha = a + b\sqrt{D},\ \beta = a - b\sqrt{D}$, where $a, b \in \mathbb{Q},\ b \neq 0,\ D$ a squarefree integer. We may further assume a, b to be rational integers and gcd$\{a, b\} = (a, b)$ is squarefree. In fact, when we replace $x,\ y$ by $x/d^2,\ y/d^3$, then the equation of $E: \ y^2 = x(x-\alpha)(x-\beta)$ becomes $E_d: \ y^2 = x(x - d^2\alpha)(x - d^2\beta)$. E and E_d are $\mathbb{Q}$-isomorphic, so $E(\mathbb{Q}) \cong E_d(\mathbb{Q})$, $E_{tors}(\mathbb{Q}) \cong E_{dtors}(\mathbb{Q})$. Our main result here is the following theorem.

THEOREM 1. *Suppose that $E: \ y^2 = x(x+M)(x+N)$ is an elliptic curve, where $M = m + n\sqrt{D},\ N = m - n\sqrt{D},\ D$ and $(m,\ n)$ are squarefree integers, $D \neq 1,\ n \neq 0$, and m are all rational integers. Then the $\mathbb{Q}$-rational torsion subgroup $E_{tors}(\mathbb{Q})$ of E is classified as follows:*

(I) $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z}$ if and only if $m = a^2 + b^2D,\ n = 2ab,$ where $a, b \in \mathbb{Z}$ are relatively prime and non-zero.

(II) $E_{tors}(\mathbb{Q}) = \mathbb{Z}/8\mathbb{Z}$ if and only if $m = u^4 + v^2w^2D,\ n = 2u^2vw,\ 2u^2 - v^2 = w^2D$, where $u, v, w \in \mathbb{Z}$ are non-zero.

(III) $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/6\mathbb{Z}$ if and only if $m = a^2 + 2ac + b^2D,\ n = 2b(a+c),\ a^2 - b^2D = c^2$, where $a, b, c \in \mathbb{Z}$ are relatively prime and non-zero.

(IV) $E_{tors}(\mathbb{Q}) = \mathbb{Z}/12\mathbb{Z}$ if and only if $m = v^2 - u^2 + w^2D,\ n = 2vw,$ and $3(v^2 - w^2D)^4 - 4v^2(v^2 - w^2D)^2(v^2 + w^2D) - 16u^4v^2w^2D = 0$, where $u, v, w \in \mathbb{Z}$

are non-zero.

(V) $E_{tors}(\mathbb{Q}) = \mathbb{Z}/10\mathbb{Z}$ *if and only if* $m = 2s(s+u)-v^2$, $n = 2st$, $(s+u)^2-v^2 = t^2D$, *and* $(u-v)^2(u+v) = 4uvs$, *where* $u, v, s, t \in \mathbb{Z}$ *are non-zero.*

(VI) Otherwise, $E_{tors}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$.

THEOREM 2. *Let* P_n *denote a generator (point) of the torsion group* $E_{tors}(\mathbb{Q})$ *of the rational points of order* n *in* E. *Then* $x(P_n)$ *and* $x(2P_n)$, *the* x*-coordinates of* P_n *and* $2P_n$ *respectively, could be as in the following, where the cases and notations are corresponding to Theorem 1:*

(I) $x(P_4) = a^2 - b^2D$; $x(2P_4) = 0$.

(II) $x(P_8) = (u+v)(v-u)^3$; $x(2P_8) = (u^2-v^2)^2$.

(III) $x(P_6) = 5c^2 + 4ac$; $x(2P_6) = c^2$.

(IV) $x(P_{12}) = (u+v)^2 - w^2D$; $x(2P_{12}) = u^2$.

(V) $x(P_{10}) = 2v^2 + 4vs - u^2$; $x(2P_{10}) = u^2$.

(VI) $x(P_2) = 0$.

II. Proofs of the Theorems

Lemma 1. *Suppose that* $E: \ y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ *is an elliptic curve over any number field* K, $\alpha, \beta, \gamma \in K$. *Let the point* $(x_0, \ y_0) \in E(K)$. *Then* $(x_0, \ y_0) = 2(x_1, \ y_1)$ *for some point* $(x_1, \ y_1) \in E(K)$ *if and only if* $x_0 - \alpha$, $x_0 - \beta$, *and* $x_0 - \gamma$ *all are squares in* K *(see [5], p85).*

Proof of Theorem 1. *By Lutz-Nagell theorem, any rational torsion point* $P \in E_{tors}(\mathbb{Q})$ *is an integer point, i.e., the coordinates* $x(P), \ y(P) \in \mathbb{Z}$ *(see [5]). The following duplication formula could be obtained from formulae of [4]:*

$$x(2P) = ((x(P)^2 - MN)/2y(P))^2. \qquad (*)$$

(I) If $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z}$, *then* E *has a rational point* P *of order 4, and* $2P = P_0 = (0,0)$ *is the unigue rational point of order 2. By Lemma 1,* M *and* N *are squares in the field* $K = \mathbb{Q}(\sqrt{D})$. *In fact we could easily see that* $M, \ N$ *are squares in the ring* $\mathbb{Z}[\sqrt{D}]$. *In other words, we have* $M = (a+b\sqrt{D})^2$, $N = (a-b\sqrt{D})^2$, $a, b \in \mathbb{Z}$. *So we have* $m = a^2 + b^2D$, $n = 2ab$. *Since* (m, n) *is squarefree and* $n \neq 0$, *so* $(a, b) = 1$, $ab \neq 0$.

Conversely, if the conditions on m, n *in (I) hold, then* M, N *are squares in* K. *By Lemma 1, there is a* K*-rational point* P *of* E *such that* $2P = P_0 = (0,0)$. *By the duplication formula (*) we have* $x(P)^2 - MN = 0$, $x(P)^2 = MN = (a^2-b^2D)^2$, $x(P) = \pm(a^2 - b^2D)$. *Substitute this* $x(P)$ *into the equation of* E, *we obtain two integer points* P: $x(P) = (a^2 - b^2D)$, $y(P) = \pm 2a(a^2 - b^2D)$ (*There is no rational point* P *with* $x(P) = -(a^2 - b^2D)$) . *These* P *are points of order 4 in* $E_{tors}(\mathbb{Q})$.

(II) Suppose that $E_{tors}(\mathbb{Q}) = \mathbb{Z}/8\mathbb{Z}$ *and* P *is a rational point of order 8 of* E. *So* $2P$ *is of order 4, and by (I) we know that* $m = a^2 + b^2D,\ n = 2ab,$ *and* $x(2P) = a^2 - b^2D$. *Then by Lemma 1 we know that* $x(2P) = a^2 - b^2D,\ x(2P) + M = 2a^2 + 2ab\sqrt{D},\ x(2P) + N = 2a^2 - 2ab\sqrt{D}$ *all are squares in field* K. *From the duplication formula (*) and the fact that* $x(P),\ y(P),\ x(2P),\ MN,\ a,$ *and* b *are rational integers, we obtain that (i)* $a^2 - b^2D = c^2$ *; (ii)* $2a^2 + 2ab\sqrt{D} = (s + t\sqrt{D})^2$*; where* $c,\ s,\ t \in \mathbb{Z}$. *These give: (iii)* $s^2 = a(a+c)$*; (iv)* $t^2D = a(a-c)$. *Since* $(a,b) = 1$ *and* D *is squarefree, from (i) we have* $(a,c) = 1$. *So* $(a, a+c) = 1$, *and via (iii) we have* $a = u^2,\ a + c = v^2$, *where* $u, v \in \mathbb{Z}$ *and* $(u,v) = 1$. *Note that* D *is squarefree, so by (iv) we have* $2u^2 - v^2 = w^2D$ *with* $w \in \mathbb{Z}$. *Then via (i) we have* $b = vw$, *so* $m = u^4 + v^2w^2D,\ n = 2u^2vw,\ 2u^2 - v^2 = w^2D$, *where* $u, v, w \in \mathbb{Z}$ *are non-zero.*

Conversely, suppose that E *satisfies the given condition. So* E *also satisfies the condition in Case (I). Thus* E *contains a* $\mathbb{Q}$*-rational point* P_4 *of order 4 with* $x(P_4) = (u^2 - v^2)^2$. *It is easy to verify that the coordinates of* P_4 *satisfy Lemma 1 for* $K = \mathbb{Q}(\sqrt{D})$. *So there is a* K*-rational point* P *with* $2P = P_4$, *and then* P *has order 8 and* $x(2P) = x(P_4) = (u^2 - v^2)^2$. *From the duplication formula (*) we have* $4y^2(u^2 - v^2)^2 = (x^2 - MN)^2$ *(here* $x = x(P)$*). Substitute the relations for* m, n *into the this equation and the equation of* E *we obtain*

$$x^4 - 4(u^2-v^2)^2x^3 - 2(u^2-v^2)^2(5u^4+6u^2v^2-3v^4)x^2 - 4(u^2-v^2)^6x + (u^2-v^2)^8 = 0,$$

which turns to be

$$(x - (u^2 - v^2)^2)^4 = 16u^4(u^2 - v^2)^2x^2,$$

having a rational-integer solution

$$x = (u+v)(v-u)^3.$$

It is easy to see that this is the only integer solution. Substituting this x *into the equation of* E, *we obtain* y *which is obviously a rational-integer. So we find a* $\mathbb{Q}$*-rational point* P_8 *of order 8, and obtain that* $x(P_8) = (u+v)(v-u)^3$. *This proves case (II).*

(III) Suppose that $E_{tors}(\mathbb{Q}) \supset \mathbb{Z}/6\mathbb{Z}$ *. Then there is a rational point of order 3 in* E, *denote it by* P. *Obviously* $x(2P) = x(P) \neq 0$. *From the duplication formula (*) we have* $x(2P) = u^2 = x(P),\ u \in \mathbb{Z}$. *By the property of torsion points with order 3 (see [6], p40), we know that x=x(P) satisfies the equation* $3x^4 + 4(M+N)x^3 + 6MNx^2 - M^2N^2 = 0$. *As a homogeneous polynomial equation of degree 4 in the variables* $M,\ N,$ *andx, it could be parametrized (due to Nigel Boston, see [3]) as* $M/x = (1+t)^2 - 1,\ N/x = (1+1/t)^2 - 1$ *for some* t. *for some* t. *Obviously* $t \in \mathbb{Q}(\sqrt{D}) - \mathbb{Q}$, *Let* $t = (a + b\sqrt{D})/c,$ *with* $(a,b,c) = 1,\ bc \neq 0,\ a, b, c \in \mathbb{Z}$. *Substituting* t *and the above* $M/x,\ N/x$ *into the equation of* E, *we have* $(2 + a/c + ac/(a^2 - b^2D))(b/c - bc/(a^2 - b^2D) = 0$. *If* $2 + a/c + ac/(a^2 - b^2D) = 0$, *then* $2 + t + 1/t = (b/c - bc/(a^2 - b^2D)\sqrt{D}$. *Substituting into the equation of* E, *we have* $(y/x)^2/x = (b/c - bc/(a^2 - b^2D)^2D$, *which is impossibe since* $x = u^2$ *and* D *is squarefree. Therefore we must have* $b/c - bc/(a^2 - b^2D) = 0,\ a^2 - b^2D = c^2$. *So* $1/t = (a - b\sqrt{D})/c$, *and we obtain*

$$m = x(a^2 + 2ac + b^2D)/c^2, \quad n = 2xab(a+c)/c^2$$

It is easy to verify that $(a^2+2ac+b^2D,\ 2b(a+c),\ c^2)$ is squarefree, which implies $x=c^2$. So $m=a^2+2ac+b^2D,\ n=2b(a+c),\ a^2-b^2D=c^2$, as desired.

Now suppose that E satisfies the given condition of (III). From the condition we could easily obtain a $\mathbb{Q}-$rational point P_3 of order 3 with $x(P_3)=c^2$ and $|y(P_3)|=2|a+c|c^2$ (Actually, every rational point of order 3 of such E satisfies $x(P_3)=c^2$). Thus $P_3+P_0=P_6$ is a non-trival $\mathbb{Q}-$rational point of order 6, where $P_0=(0,0)$ is a point of order 2. Then via the coordinate formula for the group law of an elliptic curve, we obtain $x(P_6)=5c^2+4ac$. This proves the case (III).

(IV)Suppose that $E_{tors}(\mathbb{Q})=\mathbb{Z}/12\mathbb{Z}$. Then E has a rational point P of order 12. So $2P$ has order 6. Similarly as we just proved case (II) by using some results of case (I), we could obtain the following by using results of case (III): $m=v^2-u^2+w^2D$, $n=2vw$. We thus also have (1) $b(a+c)=vw$; (2) $5c^2+4ac=u^2$; (3) $a^2-b^2D=c^2$; and (4) $4c(a+c)+(a+c)^2+b^2D=v^2+w^2D$; where a,b,c are as in case (III), and $u,v,w\in\mathbb{Z}$ are non-zero. From these formulae (1–4) and via calculation, we could obtain the desired expression

$$3(v^2-w^2D)^4-4u^2(v^2-w^2D)^2(v^2+w^2D)-16u^4v^2w^2D=0.$$

Conversely, suppose that E satisfies the given condition in (IV). Then E satisfies the condition of case (III), so E has a rational point P_6 of order 6 with $x(P_6)=5c^2+4ac=u^2$. By a method similar to that in case (II), we obtain that E has a $\mathbb{Q}(\sqrt{D})-$rational point P of order 12 and $x(P)$ satisfies the following equation:

$$x^4-4u^2x^3-hx^2-4u^2ex+e^2=0$$

where

$$h=2((v^2-w^2D)^2+2u^2(v^2+w^2D)-3u^4),$$
$$e=(v^2-w^2D)^2+u^4-2u^2(v^2+w^2D).$$

Via a careful calculation using the condition satisfied by E, we deduce the above equation as

$$((x-u^2)^2-(2u^2(v^2+w^2D)-(v^2-w^2D)^2))^2=4(v^2-w^2D)^2x^2.$$

Thus we obtain the integer solution $x=(u+v)^2-w^2D$, and then get $y=y(P)\in\mathbb{Z}$. So E has a non-trival $\mathbb{Q}-$rational point P_{12} of order 12, and $x(P_{12})=(u+v)^2-w^2D$. The case (IV) is proved.

(V) Suppose that $E_{tors}(\mathbb{Q})=\mathbb{Z}/10\mathbb{Z}$ and P is a non-trival rational point of order 5. Then it is easy to see that $x(4P)=x(P)$ and $x(2P)\neq x(P)$. Then using the duplication formula (*) as in the formal cases we could obtain that $m=2s(s+u)-v^2,\ n=2st$, and $(s+u)^2-v^2=t^2D,\ (u+v)(u-v)^2=4uvs$, where $u,v,s,t\in\mathbb{Z}$ are non-zero.

Conversely, suppose that E satisfies the condition of (V). Then from the condition it is easy to find a rational point P_5 of order 5 and obtain $x(P_5)=u^2,\ |y(P_5)|=|u(u^2-v^2+2us)|$. So $P_0+P_5=P_{10}$ is a rational point of order 10. Then via the coordinate formulae of the additive law of elliptic curves, we obtain $x(P_{10})=2v^2+4vs-u^2$. This completes the proof of Theorem 1. $\square$

In the above proof for Theorem 1, we have also proved the results of theorem 2.

References

[1] B. Mazur, Modular curves and the Eisenstein ideal, IHES Publ. Math. 47(1977), 33-186 .

[2] B. Mazur, Rational points on modular curves, Modular Functions of One Variable V, Lecture Notes in Math. 601(1977), 107-148, Springer-Verlag, New York.

[3] K. Ono, Euler's concordant forms, Acta Arithmetica, LXX VIII 2(1996), 101-123.

[4] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[5] A. knapp, Elliptic Curves, Princeton Univ. Press, Princeton, 1992.

[6] J. Silverman and J.Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York, 1992.

Department of Mathematics, Tsinghua University, Beijing 100084, P. R. China
E-mail: xianke@tsinghua.edu.cn
xzhang@math.tsinghua.edu.cn
Fax: 0086-10-62562768
(This paper was published in:
Acta Mathematica. Sinica (English Series), 18(2002.7), No.3, 539-548)